03/8043-SNY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-163853

(43)Date of publication of application : 18.06.1999

(51)Int.Cl. H04L 9/32
G06K 17/00
G07F 7/12

(21)Application number : 09-340885

(22)Date of filing : 27.11.1997

(71)Applicant : KDD

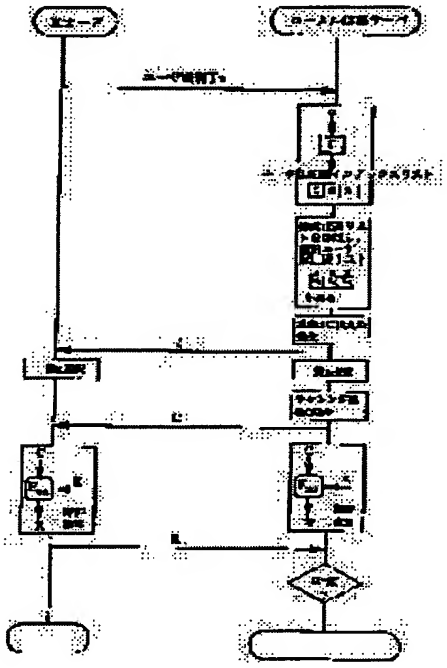
(72)Inventor : OHASHI MASAYOSHI
ISHII MASANORI

(54) AUTHENTICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To perform inquiry to plural authentication servers, to reduce manage ment cost and to improve reliability by performing authentication based on the authentication key of a user which corresponds to an optional sequence number that is decided by an authenticating means and the authentication key of the user which corresponds to a sequence number that belongs to an authenti cated means.

SOLUTION: At the time of issuing an IC card of a user i, an authentication key index list (i1 to i3) and ijε (1,...10) (j=1 to 3) of list length 3 is led from a user identifier u according to one directivity function F. When the index list is (1, 6 and 3), the authentication key list of the user i is (k1, K6 and K3). A local authentication server generates a random number jε (1 to 3) as a sequence number, and a user authentication server sends j which is the sequence number of a key list to be authenticated to the IC card and decides an authentication key. A challenge random number C is generated and it is notified to the IC card. Responses R and R are led from both the number C and the key and when they coincide, it is decided as regal.



LEGAL STATUS

[Date of request for examination] 08.09.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－163853

(43)公開日　平成11年(1999)６月18日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｖ
Ｇ０７Ｆ　7/12		Ｇ０７Ｆ　7/08	Ｂ
		Ｈ０４Ｌ　9/00	６７３Ａ
			６７５Ｂ

審査請求　未請求　請求項の数９　ＦＤ　（全８頁）

(21)出願番号　特願平9－340885

(22)出願日　平成９年(1997)11月27日

(71)出願人　000001214
ケイディディ株式会社
東京都新宿区西新宿２丁目３番２号

(72)発明者　大橋　正良
東京都新宿区西新宿２丁目３番２号国際電信電話株式会社内

(72)発明者　石井　正憲
東京都新宿区西新宿２丁目３番２号国際電信電話株式会社内

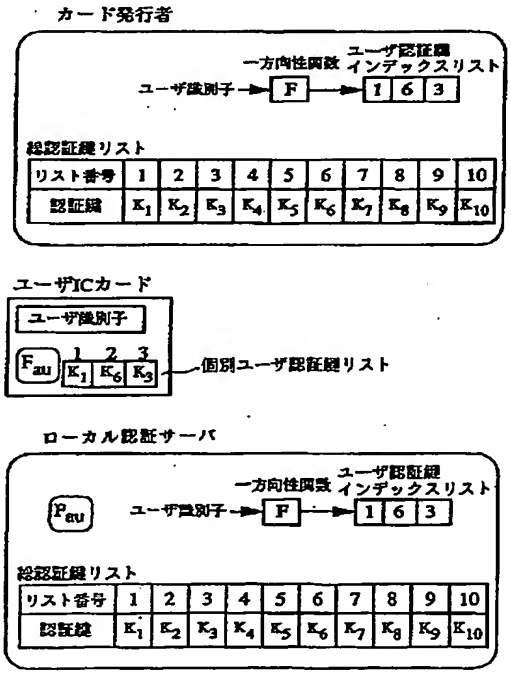
(74)代理人　弁理士　山本　恵一

(54)【発明の名称】　認証システム

(57)【要約】

【課題】　ユーザが所持するＩＣカードを認証する場合に、ローカル認証サーバへ問い合わせることで、認証のための管理コストの低減及び信頼性の向上を実現する認証システムを提供する。

【解決手段】　インデックス番号で順序づけられたｎ個の認証鍵のリストと、当該被認証手段のユーザｉに対する識別子から、ユーザ個別の系列長ｍの認証鍵インデックスリストを一意に決定するための関数Ｆとを有する認証手段と、認証鍵インデックスリストに対応したｎ個の認証鍵の部分集合となる、系列長ｍの認証鍵リストと、ユーザ識別子とを有する被認証手段とを備えており、認証手段において決定された任意の順序番号ｊに対応する認証鍵Ｋｉｊと、被認証手段が有する該順序番号ｊに対応する認証鍵Ｋｉｊ'に基づいて認証を行うものである。



【特許請求の範囲】

【請求項１】　インデックス番号で順序づけられたｎ（ｎ≧２）個の認証鍵のリスト｛$K_1,\ldots,K_n$｝と、当該認証の対象となる被認証手段のユーザｉに対する識別子から、ユーザ個別の順序づけられた系列長ｍ（ｍ≦ｎ）の認証鍵インデックスリスト｛$i_1,\ldots,i_m$｝，$i_j \in \{1,\ldots,n\}$，（ｊ＝１，．．．，ｍ）を一意に決定するための関数Ｆとを有する認証手段と、

前記認証鍵インデックスリストに対応した前記ｎ個の認証鍵の部分集合となる、順序づけられた系列長ｍ（ｍ≦ｎ）のユーザｉの認証鍵リスト｛$K_{i1},\ldots,K_{im}$｝，$K_{ij} \in \{K_1,\ldots,K_n\}$，（ｊ＝１，．．．，ｍ）と、ユーザｉに対する識別子とを有する被認証手段とを備えており、

前記認証手段において決定された任意の順序番号$j \in \{1,\ldots,m\}$に対応するユーザｉの認証鍵K_{ij}と、前記被認証手段が有する該順序番号ｊに対応するユーザｉの認証鍵K_{ij}'に基づいて認証を行うように構成されていることを特徴とする認証システム。

【請求項２】　前記関数Ｆが、一方向性関数であることを特徴とする請求項１に記載の認証システム。

【請求項３】　前記認証手段及び前記被認証手段は、同一の認証アルゴリズムF_{au}を更に備えていることを特徴とする請求項１又は２に記載の認証システム。

【請求項４】　前記認証手段がチャレンジコードを前記被認証手段へ通知し、該認証手段及び該被認証手段は、前記認証アルゴリズムF_{au}を用いて該チャレンジコードと前記認証鍵とからレスポンスコードを生成し、該認証手段は、該手段自身のレスポンスコードと、該被認証手段から通知されたレスポンスコードとを比較して認証を行うようなチャレンジーレスポンス型に構成されていることを特徴とする請求項１から３のいずれか１項に記載の認証システム。

【請求項５】　前記被認証手段がチャレンジコードを前記認証手段へ通知し、該認証手段及び該被認証手段は、前記認証アルゴリズムF_{au}を用いて該チャレンジコードと前記認証鍵とからレスポンスコードを生成し、該被認証手段は、該手段自身のレスポンスコードと、該認証手段から通知されたレスポンスコードとを比較して認証を行うようなチャレンジーレスポンス型に構成されていることを特徴とする請求項１から４のいずれか１項に記載の認証システム。

【請求項６】　前記認証手段から、前記被認証手段へ任意の順序番号ｊを通知することにより、該認証手段及び該被認証手段における該順序番号ｊに対応する認証鍵K_{ij}に基づいて認証を行うように構成されていることを特徴とする請求項１から５のいずれか１項に記載の認証システム。

【請求項７】　前記認証手段及び前記被認証手段は、前記ユーザ識別子及び時刻情報により前記順序番号ｊを生成する関数Ｈを有しており、該認証手段及び該被認証手段における該順序番号ｊに対応する認証鍵K_{ij}に基づいて認証を行うように構成されていることを特徴とする請求項１から６のいずれか１項に記載の認証システム。

【請求項８】　前記被認証手段がＩＣカードであり、前記認証手段が当該ＩＣカードリーダであることを特徴とする請求項１から５のいずれか１項に記載の認証システム。

【請求項９】　前記認証手段の認証情報がＩＣカードのようなモジュールに記憶されており、該モジュールが前記認証手段のＩＣカードリーダに取り付けることが可能であることを特徴とする請求項８に記載の認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ユーザを認証するためのシステムに関するものである。特に、通信を必要とするユーザ認証システムに有用であり、ユーザが携帯しているＩＣカード（例えばテレフォンカード）と、サービス提供者が備えているＩＣカードリーダ（例えば公衆電話機）との認証システムに関する。

【０００２】

【従来の技術】従来の認証技術の最も簡単な例として、ユーザが所持するクレジットカードにおいて、クレジットカード番号に加えて暗証番号をサービス提供者へ通知することにより認証を行うものがあった。

【０００３】また、最近、公衆型通信においても、ＩＣカードによってユーザを認証する機能が重要になってきている。特に、無線を利用する移動通信システムでは、アクセスするユーザを確認する必要があることから、ユーザ認証は必須とされている。例えば欧州標準であるＧＳＭ(Global System for Mobile Communication)ではＳＩＭ(Subscriber Identity Module)と称されるＩＣカードに加入者番号、認証鍵及び認証アルゴリズムを組み込んでユーザ認証を行っている。

【０００４】更に、信頼性の高い認証技術として、チャレンジーレスポンス型認証方式がある。これは、ある認証アルゴリズムを仮定し、ユーザの持つ認証鍵を用いて、認証サーバより乱数の投げかけ（チャレンジ）に対して、アルゴリズムの演算結果（レスポンス）を認証サーバに返して、該認証サーバがその結果を比較して確認するものである。共通鍵暗号アルゴリズムを用いたチャレンジーレスポンス型認証方式では、同一の認証鍵がユーザと認証サーバとに共有されていなければならない。前述のＧＳＭ、携帯電話システム又はコードレス電話システムでは、このチャレンジーレスポンス型認証方式が採用されている。

【０００５】

【発明が解決しようとする課題】しかし、ユーザ認証鍵の管理方式によっては、第１に認証サーバの管理コスト、及び第２にローカル認証サーバの信頼性において問

題がある。

【０００６】第１に、認証サーバの管理コストにおける問題を説明する。ユーザ認証として、最も確実な構成は、１つの認証サーバがユーザの全ての認証情報を記憶するデータベースを有していることである。ユーザ認証が発生するごとに該認証サーバにユーザ認証情報を問い合わせなければならない。従って、この構成は、ユーザ情報を安全に且つ確実に管理することができるが、ユーザが利用する端末から認証サーバへのアクセスコスト及び時間を必要とするという問題がある。また、全てのユーザが直接、１つの認証サーバへアクセスすることができると、不正なアクセスを厳しくチェックする必要があり、認証サーバの管理コストも増大することとなる。認証サーバが集中して認証を行うものとして、例えばＰＨＳ(Personal Handy phone System) がある。

【０００７】このような、１つの認証サーバを備えることの不都合な点を回避するために、複数のローカル認証サーバを備え、該ローカル認証サーバのみでユーザ認証を行うという方法もある。

【０００８】第２に、ローカル認証サーバを備えた場合の信頼性における問題を説明する。最も簡単な方法は、システム全体、つまりユーザ全員に同じ認証鍵を渡すものである。これは一人の認証鍵が露呈するとシステム全体のセキュリティが無くなる危険性がある。

【０００９】次の方法として、例えばユーザ識別子のような情報に基づいて、あるアルゴリズムを通すことにより、ユーザ個々の認証鍵を作成する方法がある。この方法を用いると少なくとも各ユーザに割り当てられる認証鍵は異なる。しかしながら、アルゴリズムが露呈してしまうとやはりシステム全体のセキュリティが破壊されてしまう問題が生じる。

【００１０】最も極端な例として、ローカル認証サーバに全てのユーザの認証鍵を保持する（ホームデータベースのコピーを持つ）ようにすれば、ホームへのアクセスは不要となるが、このためにはローカルサーバデータベースの維持管理に係るコストが膨大となり、現実的ではない。

【００１１】そこで、本発明は、ユーザが所持するＩＣカードを認証する場合に、システム内で１つの認証サーバに問い合わせることなく、複数のローカル認証サーバへ問い合わせることが可能であり、認証のための管理コストの低減及び信頼性の向上を実現する認証システムを提供する。

【００１２】

【課題を解決するための手段】本発明は、インデックス番号で順序づけられたｎ（ｎ≧２）個の認証鍵のリスト｛$K_1,\ldots,K_n$｝と、当該認証の対象となる被認証手段のユーザｉに対する識別子から、ユーザ個別の順序づけられた系列長ｍ（ｍ≦ｎ）の認証鍵インデックスリスト｛$i_1,\ldots,i_m$｝，$i_j \in \{1,\ldots,n\}$，（$j=1,\ldots,m$）を一意に決定するための関数Ｆとを有する認証手段と、認証鍵インデックスリストに対応したｎ個の認証鍵の部分集合となる、順序づけられた系列長ｍ（ｍ≦ｎ）のユーザｉの認証鍵リスト｛$K_{i1},\ldots,K_{im}$｝，$K_{ij} \in \{K_1,\ldots,K_n\}$，（$j=1,\ldots,m$）と、ユーザｉに対する識別子とを有する被認証手段とを備えており、認証手段において決定された任意の順序番号$j \in \{1,\ldots,m\}$に対応するユーザｉの認証鍵K_{ij}と、被認証手段が有する該順序番号ｊに対応するユーザｉの認証鍵K_{ij}'に基づいて認証を行うように構成されているものである。

【００１３】これにより、システム内で１つの認証サーバへの問い合わせを行うことなく、複数の認証手段（ローカルな認証サーバ）のみで認証を行うことが可能となり、管理コストの低減が実現できる。また、認証毎にユーザ認証鍵を換えることが可能であるので、信頼性が向上できる。

【００１４】仮に、認証手段と被認証手段との間の情報のやりとりが盗み取られ、ユーザ識別子と認証鍵の鍵の順序番号が解読されたとしても、認証鍵そのものは解読されない。また、１ユーザのＩＣカードの情報が全て解読されたとしても、それはｍ個（≦ｎ）に留まり、ｎ－ｍ個の鍵は解読されない。そのために、解読されたＩＣカード以外のＩＣカードについては、依然として本システムに使用できない。

【００１５】本発明の他の実施形態によれば、関数Ｆが、一方向性関数であるのが好ましい。一方向性関数とは、該関数の演算が高速に行えるのに対して、逆関数の演算が極めて難しい演算のことである。

【００１６】本発明の他の実施形態によれば、認証手段及び被認証手段は、同一の認証アルゴリズムF_{au}を更に備えているのが好ましい。また、認証手段がチャレンジコードを被認証手段へ通知し、該認証手段及び該被認証手段は、認証アルゴリズムF_{au}を用いて該チャレンジコードと認証鍵とからレスポンスコードを生成し、該認証手段は、該手段自身のレスポンスコードと、該被認証手段から通知されたレスポンスコードとを比較して認証を行うようなチャレンジーレスポンス型に構成されているのも好ましい。更に、被認証手段がチャレンジコードを認証手段へ通知し、該認証手段及び該被認証手段は、認証アルゴリズムF_{au}を用いて該チャレンジコードと認証鍵とからレスポンスコードを生成し、該被認証手段は、該手段自身のレスポンスコードと、該認証手段から通知されたレスポンスコードとを比較して認証を行うようなチャレンジーレスポンス型に構成されているのも好ましい。本発明を一方向又は双方向にチャレンジーレスポンス型に構成することにより、認証シーケンスの信頼性が向上する。

【００１７】本発明の他の実施形態によれば、認証手段から、被認証手段へ任意の順序番号ｊを通知することに

より、該認証手段及び該被認証手段における該順序番号ｊに対応する認証鍵Ｋｉｊに基づいて認証を行うように構成されている。これにより、認証鍵が常に一定のものとなることがなく、時間等に応じて認証鍵が異なるために、信頼性の向上につながる。

【００１８】本発明の他の実施形態によれば、認証手段及び被認証手段は、ユーザ識別子及び時刻情報により順序番号ｊを生成する関数Ｈを有しており、該認証手段及び該被認証手段における該順序番号ｊに対応する認証鍵Ｋｉｊに基づいて認証を行うように構成されている。これにより、認証鍵の順序番号を通知しないために、認証手段と被認証手段との間をモニタされることがなく、信頼性の向上につながる。

【００１９】本発明の他の実施形態によれば、被認証手段がＩＣカードであり、認証手段が当該ＩＣカードリーダである。また、認証手段の認証情報が、ＩＣカードのようなモジュールになっており、認証手段のＩＣカードリーダに取り付けることも可能である。これにより、認証情報の更なる秘匿化が実現できる。

【００２０】

【発明の実施の形態】以下、図面を用いて本発明の実施形態を詳細に説明する。

【００２１】図１は、本発明の構成図である。本発明におけるシステム構成は、ユーザが所持するＩＣカードと、ユーザ毎に割り当てられたユーザ識別子を用いて該ＩＣカードを発行するカード発行者と、該ＩＣカードと認証を行うことが可能なローカル認証サーバとからなる。従って、従来、システム内の全てのユーザのＩＣカード情報を管理するような唯一の認証サーバを必要としない。

【００２２】図２は、本発明の各構成要素の記憶情報の内容を示したものである。

【００２３】カード発行者は、システム内で使用される全てのユーザ認証鍵をインデックス番号で順序づけた総認証鍵リスト｛$K_1,\ldots,K_{10}$｝と、一方向性関数Ｆとを有している。インデックス番号ｉ（１≦ｉ≦１０）に対し認証鍵K_iが参照される。該一方向性関数とは、出力値から入力値を推定することが困難な関数であり、入力の意図的な改竄で同一の出力値を生成させることが困難な関数である。このような一方向性関数としては、ＭＤ５やＳＨＡなどのハッシュ関数が代表的な例として挙げられる。ユーザ認証鍵の総数ｎは任意であり、本例では仮にｎ＝１０としている。該カード発行者は、ユーザＩＣカードを発行する際にこれらの情報を必要とする。該カード発行者は、ＩＣカードを発行するユーザの識別子を、一方向性関数に通すことにより、ユーザ個別の順序づけられた系列長ｍの認証鍵インデックスリスト｛$i_1,\ldots,i_m$｝，$i_j \in \{1,..,n\}$，（ｊ＝$1,..,m$）を導き出す。ここではｍ＝３とした。

【００２４】ユーザＩＣカードは、ユーザ識別子と、カード発行者により書き込まれたユーザｉの認証鍵リスト｛K_{i1}，K_{i2}，K_{i3}｝，$K_{ij} \in \{K_1,\ldots,K_{10}\}$，（ｊ＝１，２，３）と、認証アルゴリズムＦauとを有している。

【００２５】ローカル認証サーバは、カード発行者が備える記憶情報に加えて、更に認証アルゴリズムＦauを有している。

【００２６】カード発行者及びローカル認証サーバとに具備される一方向性関数、認証鍵リスト、認証アルゴリズムＦauは、外部からののぞき見などの攻撃に対して耐えられるものである必要がある。例えば、専用のＩＣカードのような物理攻撃に耐え得るモジュールにこれら情報を記憶させ、該モジュールをカード発行者とローカル認証サーバとに接続するという構成がある。特に、総認証鍵リストが露見すると本発明のセキュリティが崩壊するため、全ての鍵が格納されたローカルサーバの鍵リストは厳重に管理される必要がある。

【００２７】図３は、カード発行者によるＩＣカードの発行シーケンスを表している。あるユーザi 宛のＩＣカードを発行する際に、一方向性関数Ｆにより、該ユーザのユーザ識別子ｕから系列長３の認証鍵インデックスリスト｛i_1，i_2，i_3｝，$i_j \in \{1,..,10\}$，（ｊ＝１，２，３）を導き出すことができる。この場合の認証鍵インデックスリストが｛１、６、３｝であったとすると、ユーザｉの認証鍵リストは、｛K_1、K_6、K_3｝であることを示している。カード発行者は、総認証鍵リスト｛$K_1,\ldots,K_{10}$｝から、認証鍵リスト｛K_1、K_6、K_3｝を生成し、ＩＣカードにユーザ識別子とともに書き込む。

【００２８】図４は、ユーザの所持するＩＣカードとローカル認証サーバとの間の認証シーケンスを表している。被認証手段であるＩＣカードを、認証手段であるローカル認証サーバに接続することにより、該認証シーケンスが行われる。

【００２９】最初に、ＩＣカードからローカル認証サーバへユーザ識別子ｕを通知する。ローカル認証サーバは、前述したカード発行処理手順と同じ処理手順を実行することにより、対象となるＩＣカードの個別ユーザ認証鍵リスト｛K_1、K_6、K_3｝を導き出す。

【００３０】次に、ローカル認証サーバは、順序番号として乱数ｊ∈｛１、２、３｝を発生させる。これは、ＩＣカードが有する個別ユーザ認証鍵リストと、ローカル認証サーバが導き出したユーザ認証鍵リストとにおいて、何番目の認証鍵で認証するかを示すものである。つまり、ユーザ認証サーバが、認証すべき鍵リストの順序番号であるｊをＩＣカードへ送ることにより、認証鍵が定まる。例えばｊ＝２を通知すると、ＩＣカードとローカル認証サーバとの間で用いられる鍵はK_6となる。

【００３１】次に、ローカル認証サーバは、従来のチャレンジーレスポンス型認証方式によって用いられている

チャレンジ乱数Ｃを発生させ、該ＣをＩＣカード側へ通知する。

【００３２】次に、ＩＣカード及びローカル認証サーバの両方は、認証アルゴリズムF_{au}を用いて、チャレンジ乱数Ｃ及び選択された鍵（この場合、K_6）からレスポンスを導き出す。ここでは、ＩＣカードが導き出したレスポンスをＲとし、ローカル認証サーバが導き出したレスポンスをＲ′として表している。

【００３３】最後に、ＩＣカードで導き出されたレスポンスＲがローカル認証サーバへ通知され、該ローカル認証サーバは、それ自身のレスポンスＲ′と通知されたレスポンスＲとを比較する。両レスポンスが一致すれば正当なユーザと判断され、一致しなければ不正なユーザと判断される。

【００３４】また、前述した実施形態では、順序番号ｊを明示的にローカル認証サーバからユーザに示しているが、本発明の他の実施形態では、ＩＣカードとローカル認証サーバとが同一の他の関数（例えばハッシュ関数）Ｈを用いて、最初に通知されるユーザ識別子に現時刻や宛先番号を結合する等の両者間で一致するがアクセスごとにその値が変化するようなサービス情報ｖから、ｊ＝Ｈ（ｖ）として導き出すことも可能である。これにより、図４の認証シーケンスにおいて、ローカル認証サーバから順序番号ｊを通知する必要がなくなる。

【００３５】更に、前述した実施形態では、チャレンジーレスポンス型認証方法を用いているが、本発明の他の実施形態では、認証鍵をそのまま示すパスワード方式にも適用することが可能である。

【００３６】図５は、ローカル認証サーバがＩＣカードを認証するのみならず、更にＩＣカードがローカル認証サーバを認証する相互認証シーケンスを表している。前述した図４の認証シーケンスにおける最終段階で、ＩＣカードは、ローカル認証サーバへレスポンスＲを通知する際に、チャレンジ乱数Ｃ２を新たに発生させてローカル認証サーバへ通知することにより行う。

【００３７】前述の説明では本発明の認証システムの一実施形態として、ＩＣカードとＩＣカードリーダとの間の認証を例としたが、様々な認証システムにおける適用について、本発明の技術思想及び見地の範囲の種々の変更、修正及び省略は、当業者によれば容易に行うことができる。従って、前述の説明はあくまで例であって、何ら制約しようとするものではない。本発明は、特許請求の範囲及びその等価物として限定するものにのみ制約される。

【００３８】

【発明の効果】以上、詳細に説明したように、本発明によれば、システム内で１つの集中的な認証サーバへの問い合わせを行うことなく、ローカルな認証サーバのみで認証を行うことが可能となり、管理コストの低減が実現できる。また、認証毎にユーザ認証鍵を換えることが可能であり、認証の信頼性を向上することができる。

【００３９】仮に、認証手段と被認証手段との間の情報のやりとりが盗み取られ、ユーザｉの識別子ｕと認証鍵の鍵の順序番号ｊが解読されたとしても、用いられた認証鍵K_{ij}そのものは解読されない。また、たとえ１ユーザのＩＣカードの情報が全て解読されたとしても、それはｍ個（≦ｎ）の認証鍵リスト｛$K_{i1}, \ldots, K_{im}$｝に留まり、ｎ－ｍ個の認証鍵は解読されない上、一方向性関数Ｆが依然として未知なため、これら鍵の配置情報も解読されない。そのために、解読されたＩＣカード以外のＩＣカードについては、依然として本システムに使用できないとう利点がある。

【００４０】本発明による認証システムは、システム内に１つの認証サーバではなくローカル認証サーバであっても、以上説明した特別の構成を有することにより、セキュリティを向上させることができるという格別な効果を提供するものである。

【図面の簡単な説明】

【図１】本発明の構成図である。

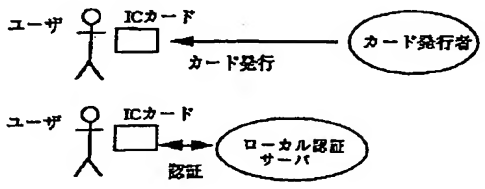
【図２】本発明の構成要素の記憶情報を示す構成図である。

【図３】本発明のＩＣカード発行シーケンス図である。

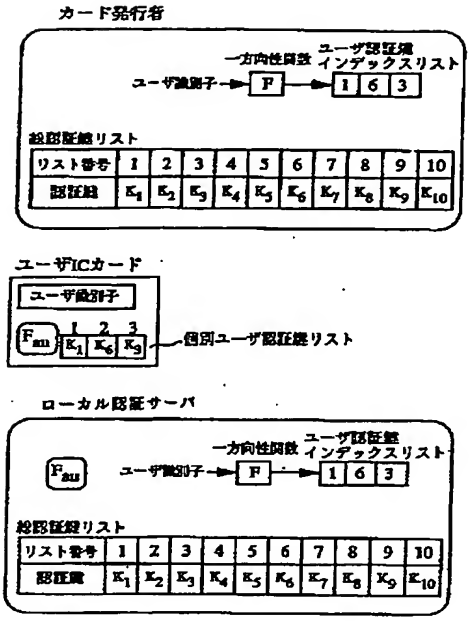
【図４】本発明のユーザ認証シーケンス図である。

【図５】本発明の相互認証シーケンス図である。

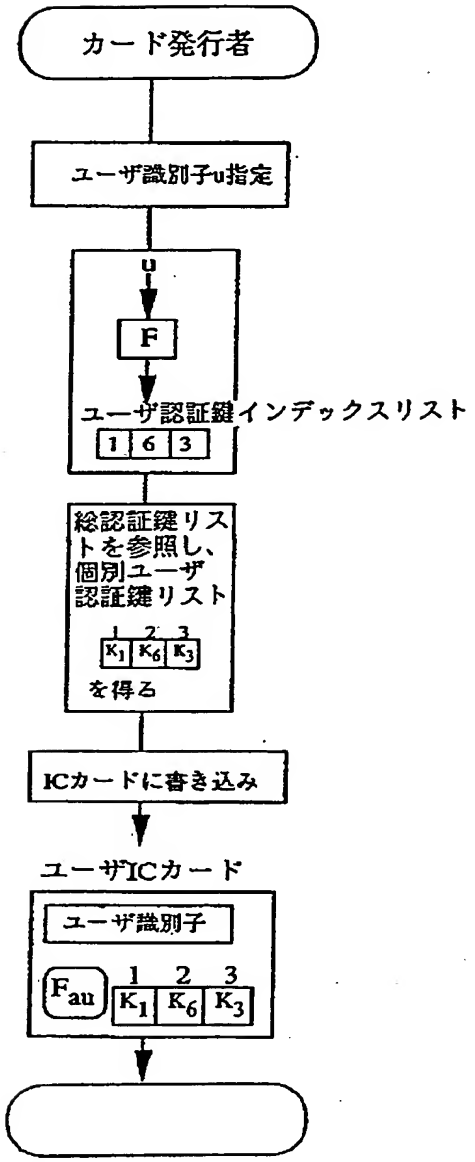
【図１】



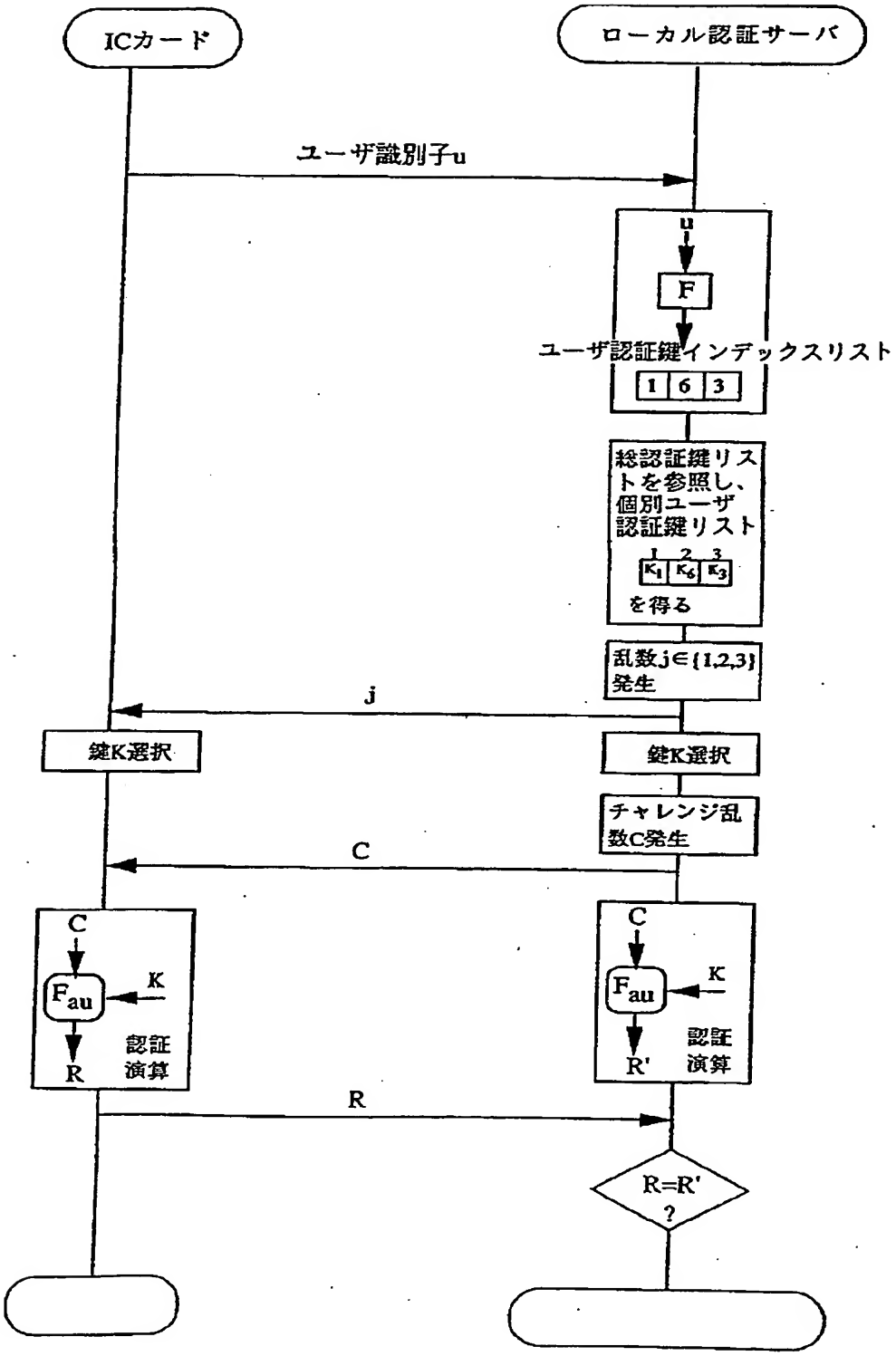
【図２】


カード発行者
一方向性関数
ユーザ認証鍵インデックスリスト
ユーザ識別子
F
1 6 3
総認証鍵リスト
リスト番号 1 2 3 4 5 6 7 8 9 10
認証鍵 K1 K2 K3 K4 K5 K6 K7 K8 K9 K10
ユーザICカード
ユーザ識別子
Fau
1 2 3
K1 K6 K3
個別ユーザ認証鍵リスト
ローカル認証サーバ
Fau
一方向性関数
ユーザ認証鍵インデックスリスト
ユーザ識別子
F
1 6 3
総認証鍵リスト
リスト番号 1 2 3 4 5 6 7 8 9 10
認証鍵 K1 K2 K3 K4 K5 K6 K7 K8 K9 K10

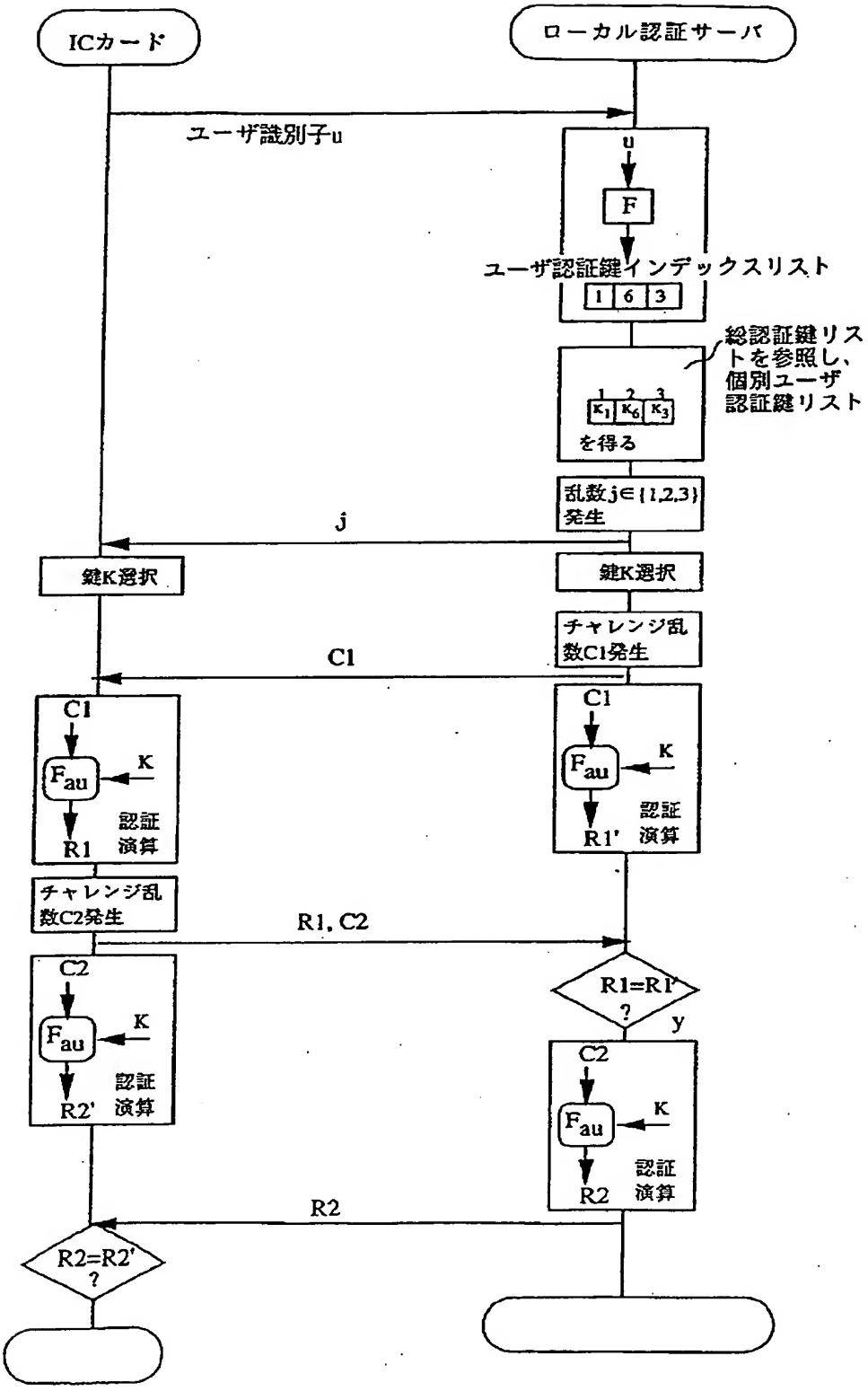
【図３】


カード発行者
ユーザ識別子u指定
u
F
ユーザ認証鍵インデックスリスト
1 6 3
総認証鍵リストを参照し、個別ユーザ認証鍵リスト
1 2 3
K1 K6 K3
を得る
ICカードに書き込み
ユーザICカード
ユーザ識別子
Fau
1 2 3
K1 K6 K3

【図４】


ICカード
ローカル認証サーバ
ユーザ識別子u
u
F
ユーザ認証鍵インデックスリスト
1 6 3
総認証鍵リストを参照し、個別ユーザ認証鍵リスト
1 2 3
K1 K6 K3
を得る
乱数j∈{1,2,3}発生
j
鍵K選択
鍵K選択
チャレンジ乱数C発生
C
C
C
K
Fau
認証演算
R
C
K
Fau
認証演算
R'
R
R=R'
?

【図５】


ICカード
ローカル認証サーバ
ユーザ識別子u
u
F
ユーザ認証鍵インデックスリスト
1 6 3
総認証鍵リストを参照し、個別ユーザ認証鍵リスト
1 2 3
K1 K6 K3
を得る
乱数j∈{1,2,3}発生
j
鍵K選択
鍵K選択
チャレンジ乱数C1発生
C1
C1
Fau
K
認証演算
R1
C1
Fau
K
認証演算
R1'
チャレンジ乱数C2発生
R1, C2
C2
Fau
K
認証演算
R2'
R1=R1'
?
y
C2
Fau
K
認証演算
R2
R2
R2=R2'
?